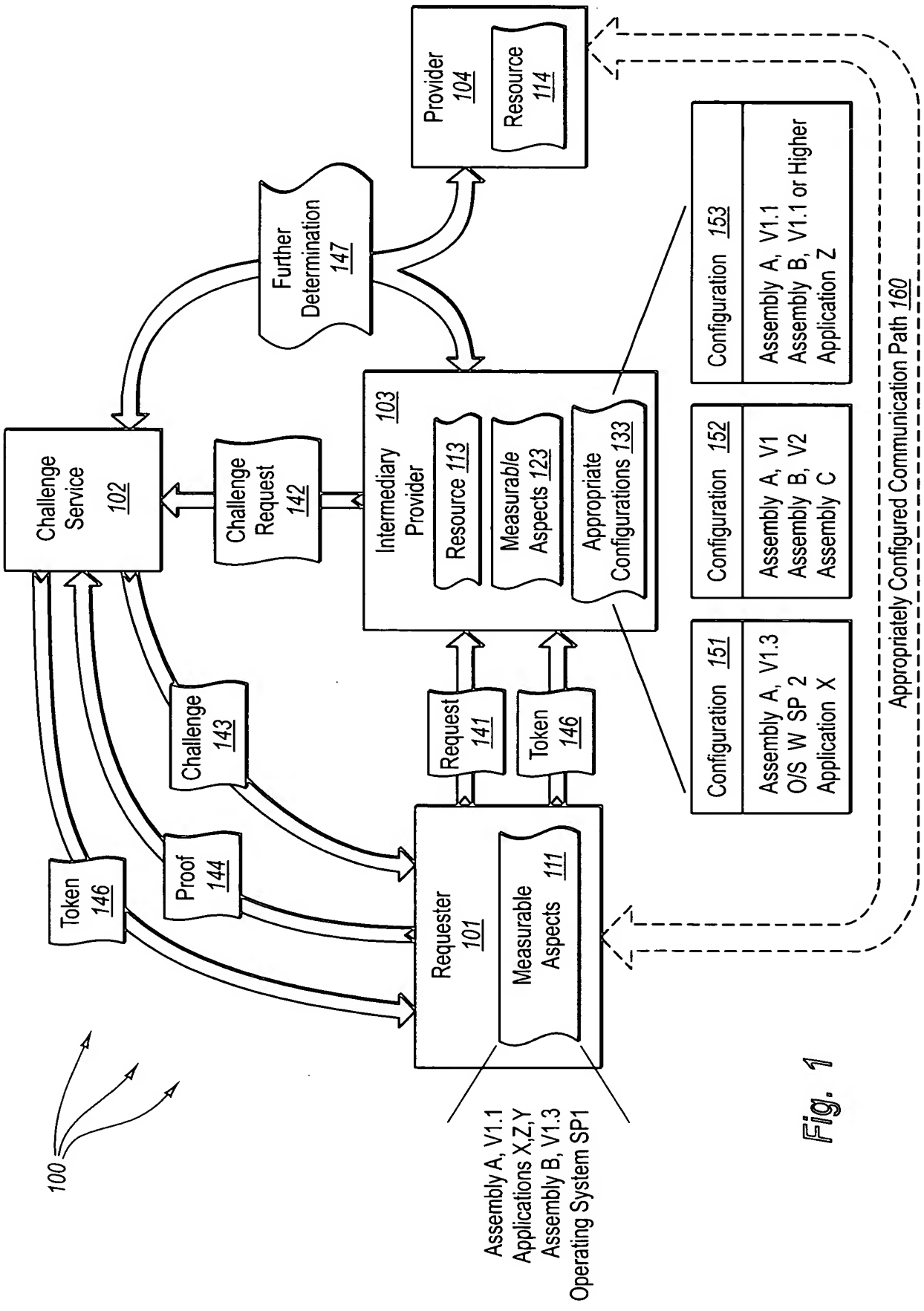
Provider 104
Resource 114
Further Determination 147
Challenge Service 102
Challenge Request 142
Intermediary Provider 103
Resource 113
Measurable Aspects 123
Appropriate Configurations 133
Configuration 153
Assembly A, V1.1
Assembly B, V1.1 or Higher
Application Z
Configuration 152
Assembly A, V1
Assembly B, V2
Assembly C
Configuration 151
Assembly A, V1.3
O/S W SP 2
Application X
Challenge 143
Request 141
Token 146
Proof 144
Token 146
Requester 101
Measurable Aspects 111
Appropriately Configured Communication Path 160
100
Assembly A, V1.1
Applications X,Z,Y
Assembly B, V1.3
Operating System SP1

Fig. 1

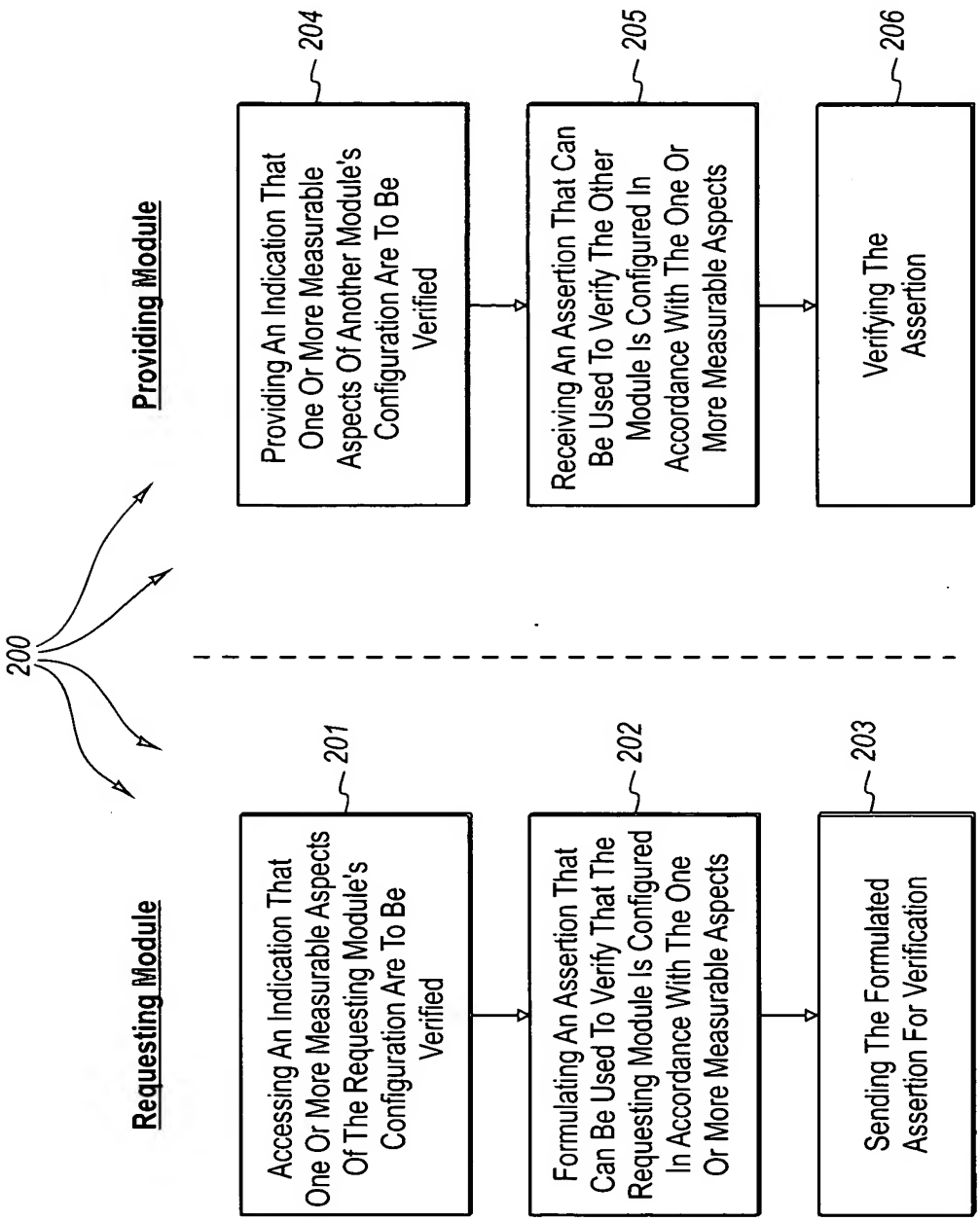
200
Requesting Module
Providing Module
201
Accessing An Indication That One Or More Measurable Aspects Of The Requesting Module's Configuration Are To Be Verified
202
Formulating An Assertion That Can Be Used To Verify That The Requesting Module Is Configured In Accordance With The One Or More Measurable Aspects
203
Sending The Formulated Assertion For Verification
204
Providing An Indication That One Or More Measurable Aspects Of Another Module's Configuration Are To Be Verified
205
Receiving An Assertion That Can Be Used To Verify The Other Module Is Configured In Accordance With The One Or More Measurable Aspects
206
Verifying The Assertion

Fig. 2

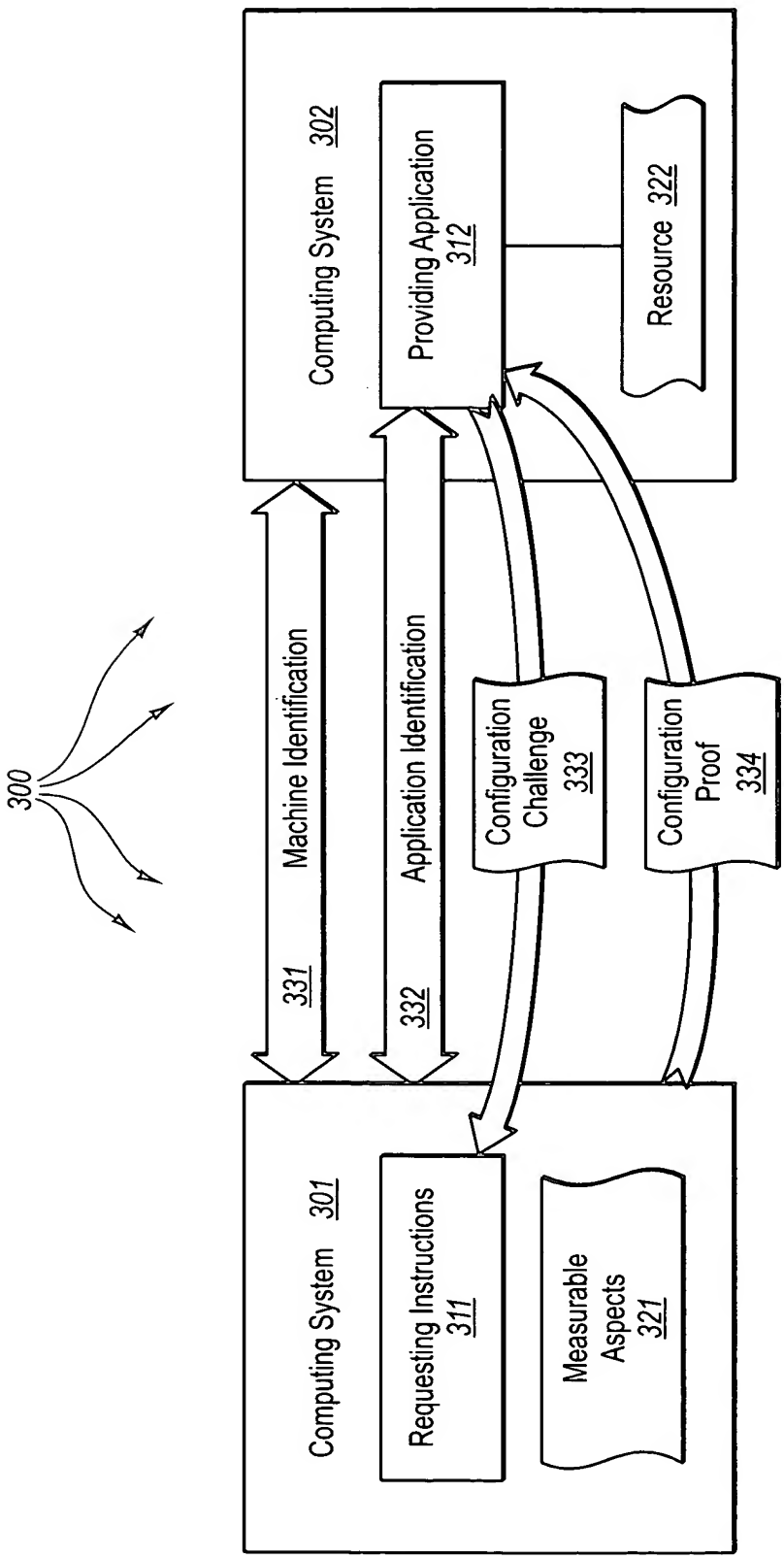
Computing System 302
Providing Application 312
Resource 322
300
Machine Identification
331
Application Identification
332
Configuration Challenge 333
Configuration Proof 334
Computing System 301
Requesting Instructions 311
Measurable Aspects 321

Fig. 3

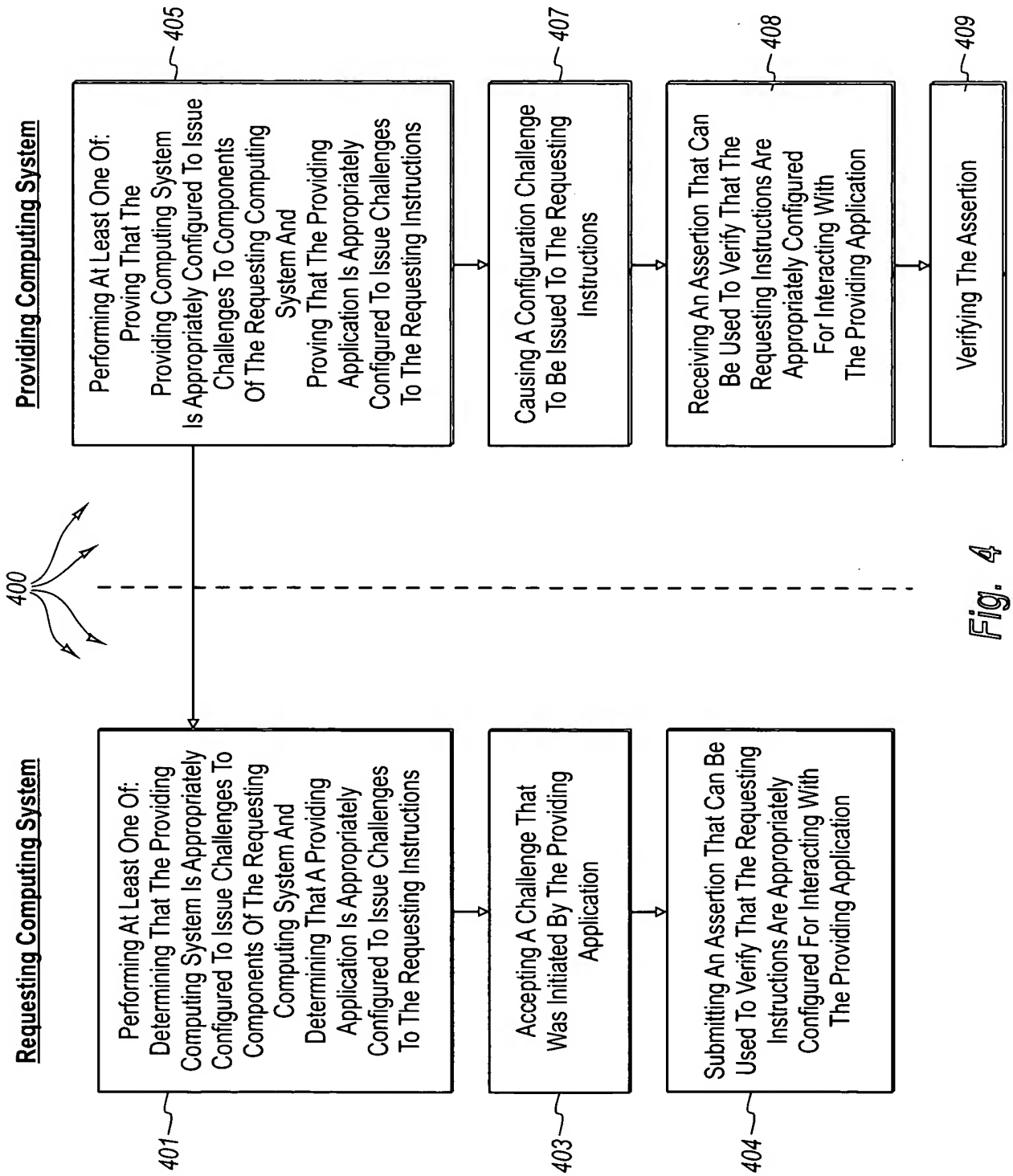
Providing Computing System
Requesting Computing System
400
401
Performing At Least One Of: Determining That The Providing Computing System Is Appropriately Configured To Issue Challenges To Components Of The Requesting Computing System And Determining That A Providing Application Is Appropriately Configured To Issue Challenges To The Requesting Instructions
403
Accepting A Challenge That Was Initiated By The Providing Application
404
Submitting An Assertion That Can Be Used To Verify That The Requesting Instructions Are Appropriately Configured For Interacting With The Providing Application
405
Performing At Least One Of: Proving That The Providing Computing System Is Appropriately Configured To Issue Challenges To Components Of The Requesting Computing System And Proving That The Providing Application Is Appropriately Configured To Issue Challenges To The Requesting Instructions
407
Causing A Configuration Challenge To Be Issued To The Requesting Instructions
408
Receiving An Assertion That Can Be Used To Verify That The Requesting Instructions Are Appropriately Configured For Interacting With The Providing Application
409
Verifying The Assertion

Fig. 4

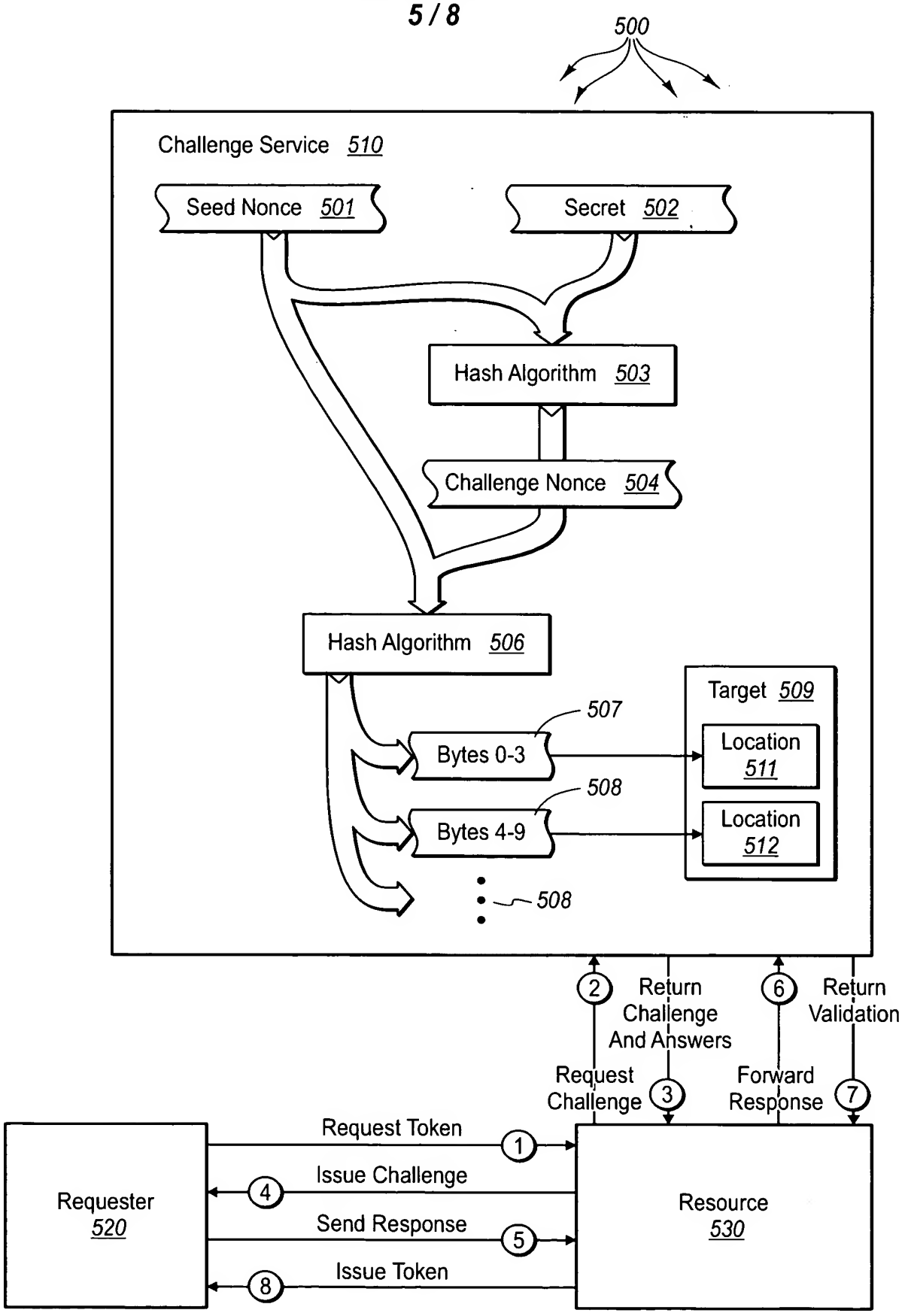
500
Challenge Service 510
Seed Nonce 501
Secret 502
Hash Algorithm 503
Challenge Nonce 504
Hash Algorithm 506
Target 509
507
Bytes 0-3
Location 511
508
Bytes 4-9
Location 512
508
2
Return Challenge And Answers
6
Return Validation
Request Challenge
3
Forward Response
7
Request Token
1
Issue Challenge
4
Send Response
5
Issue Token
8
Requester 520
Resource 530

Fig. 5

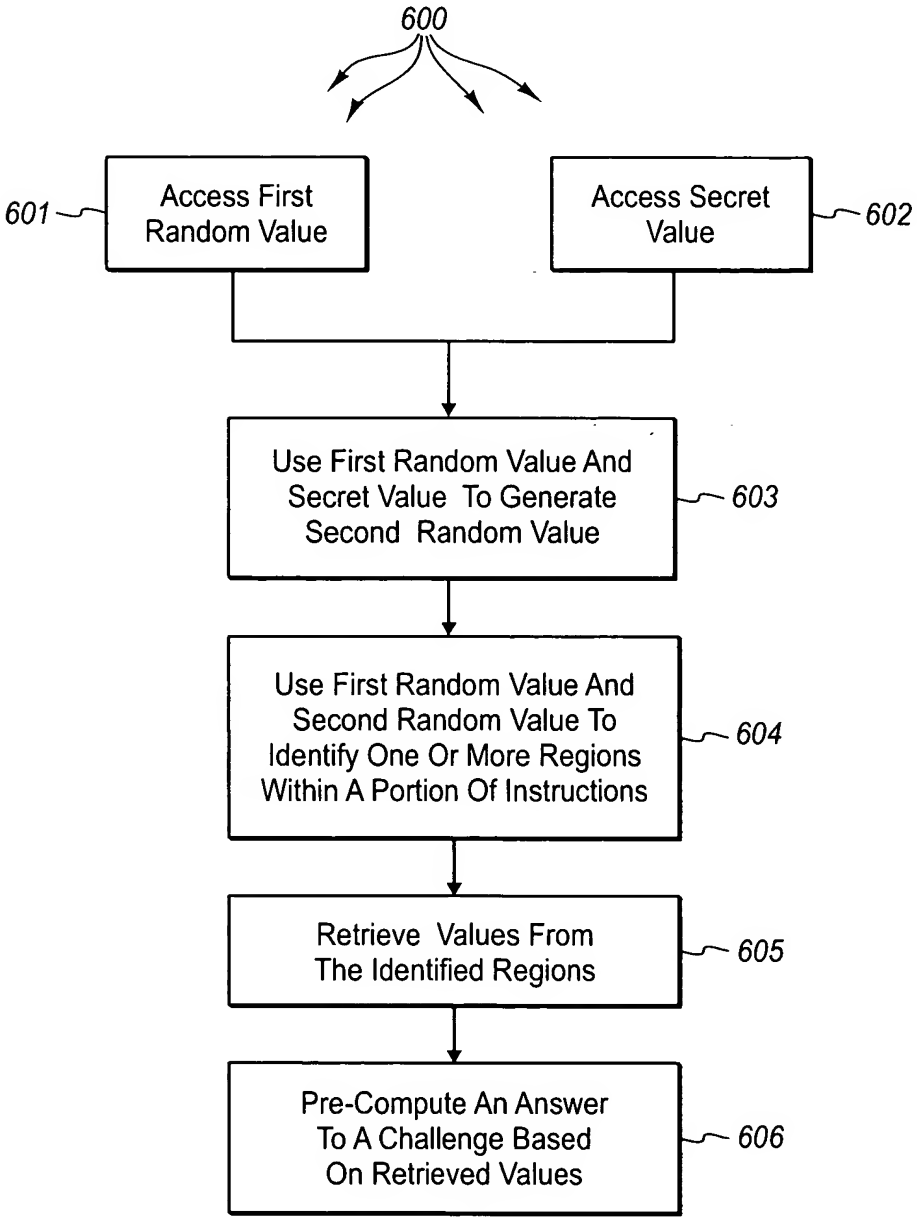
600
601
Access First Random Value
Access Secret Value
602
Use First Random Value And Secret Value To Generate Second Random Value
603
Use First Random Value And Second Random Value To Identify One Or More Regions Within A Portion Of Instructions
604
Retrieve Values From The Identified Regions
605
Pre-Compute An Answer To A Challenge Based On Retrieved Values
606

Fig. 6

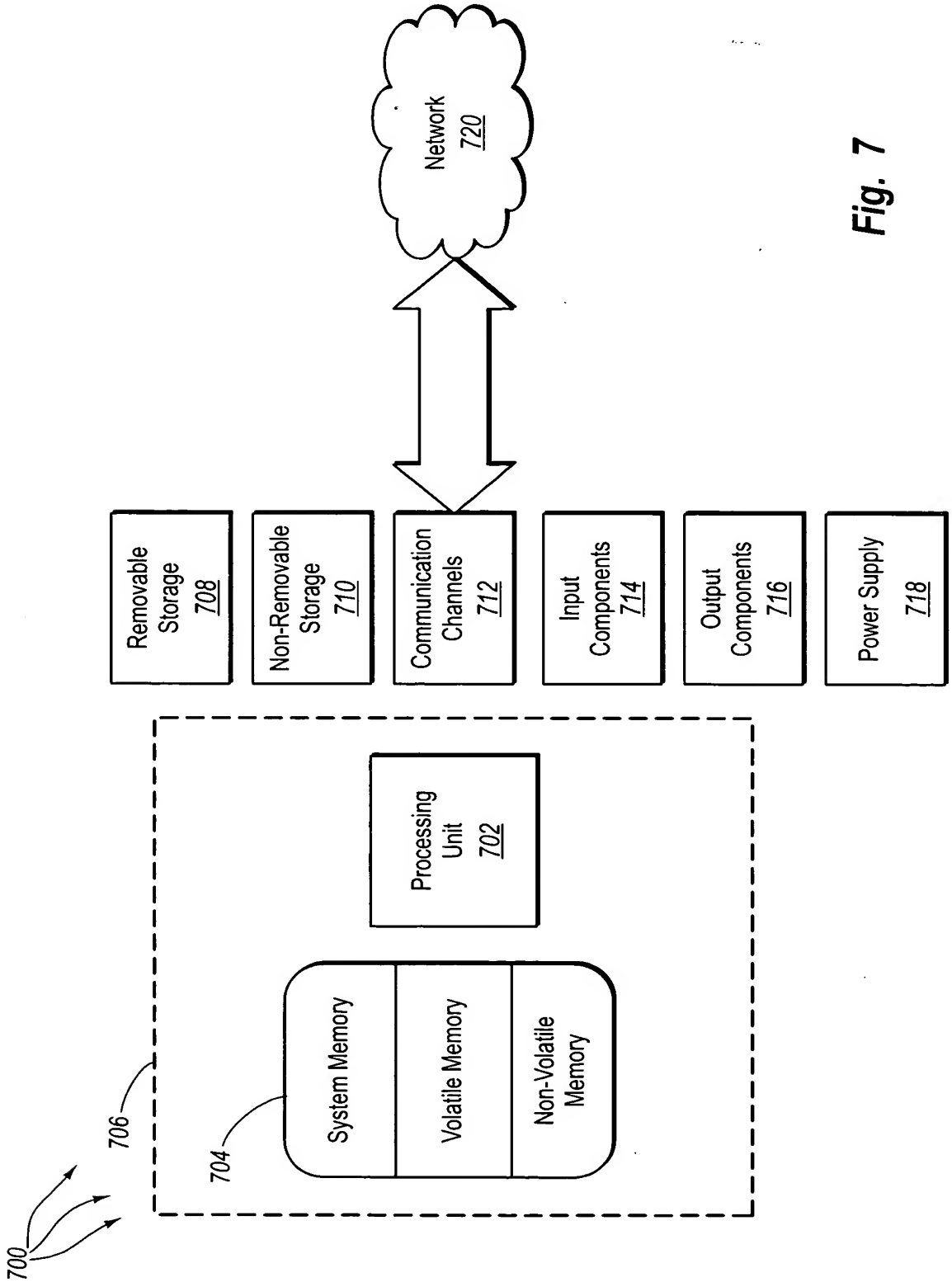
Network 720
Removable Storage 708
Non-Removable Storage 710
Communication Channels 712
Input Components 714
Output Components 716
Power Supply 718
Processing Unit 702
System Memory
Volatile Memory
Non-Volatile Memory
704
706
700

Fig. 7

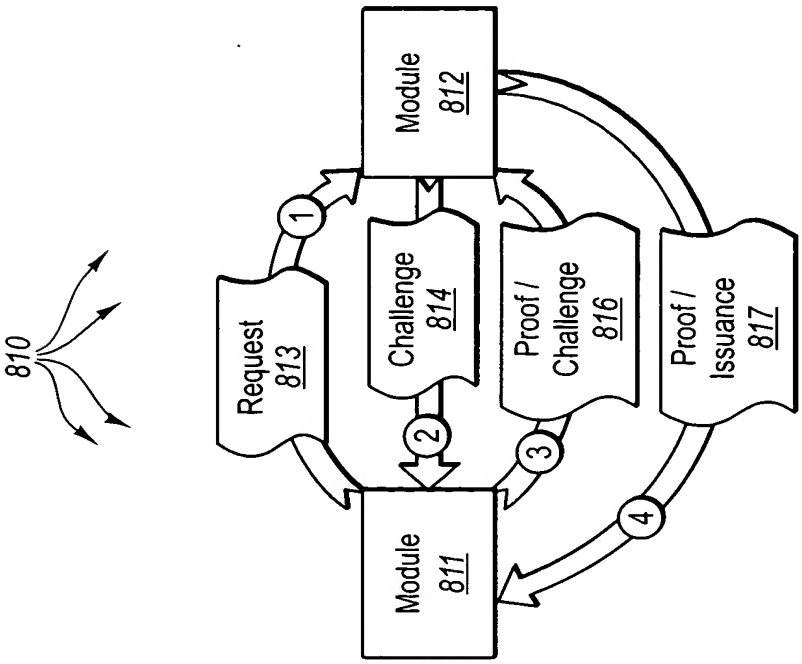
810
Module 812
Request 813
Challenge 814
Proof / Challenge 816
Proof / Issuance 817
Module 811
1
2
3
4

Fig. 8B

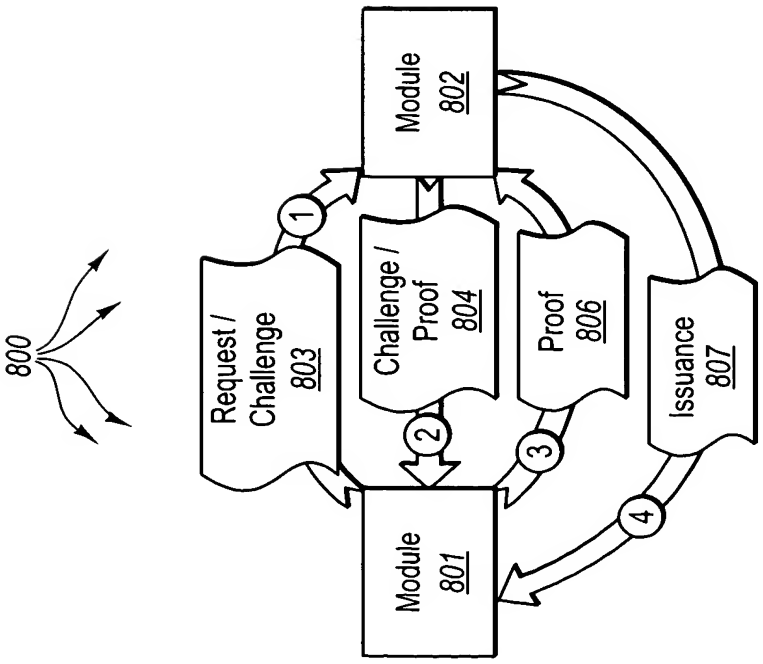
800
Module 802
Request / Challenge 803
Challenge / Proof 804
Proof 806
Issuance 807
Module 801
1
2
3
4

Fig. 8A